BAB V

PENUTUP

5.1 Kesimpulan

Dari penelitian yang dilakukan maka dapat disimpulkan sebagai berikut :

1. Penggunaan Simbol (‘) pada saat melakukan serangan SQL *Injection* dapat diatasi dengan melakukan *filter* terhadap parameter yang masuk dan dapat menjadi akses ke *database*
2. Celah keamanan XSS terjadi karena filter setiap parameter dan izin inputan berupa simbol HTML, *encode* setiap *input* dan *output*.
3. Celah keamanan CSRF terjadi karena tidak adanya penggunaan CSRF *token* disetiap *form action* yang mengakibatkan setiap melakukan *request* dapat dilakukan lebih dari sekali.
4. Pengujian hanya terbatas pada celah keamanan yang sering ditemui.
5. Keamanan dari suatu aplikasi *website* tidak selamanya dari *tools* maupun teknologi yang digunakan melainkan juga dari kejelian pengembang untuk melihat setiap celah yang ada walaupun sangat kecil

5.2 Saran

Penelitan ini masih memiliki kekurangan untuk lebih mengembangkan penelitian ini maka disarankan:

1. Melakukan langkah perbaikan dari setiap celah keamanan yang ditemukan.
2. Mencari *vulnerable* dari framework *codeigniter* selain dari SQL Injection, *Cross Site Request Forgery* (CSRF) dan *Cross Site Scripting* (XSS)